Synchronization and graph endomorphisms

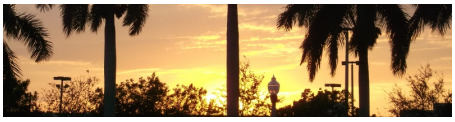
Peter J. Cameron
University of St Andrews / Queen Mary University of London

44th Southeastern Conference on
Combinatorics, Graph Theory and Computing
8 March 2013

St Andrews

As from last Friday, I am a part-time Professor of Mathematics and Statistics at the University of St Andrews.
It was during a previous visit to St Andrews that the connection between synchronization and graph endomorphisms came to me during a sleepless night.

Synchronization



A few combinatorial problems . . .

- Do there exist analogues of the Erdős–Ko–Rado Theorem and Baranyai's Theorem over "fields with more than one element", that is, with *vector space* and *subspace* replacing *set* and *subset*? (The analogue of Baranyai would ask for a partition of the k-dimensional subspaces of an n-dimensional vector space into spreads, each spread containing every non-zero vector once.)
- Which polar spaces have ovoids, spreads, or partitions into ovoids?
- For which n can we partition the k-element subsets of an n-set into Steiner systems $S(3,4,n)$, or into Steiner systems $S(2,4,n)$?

. . . which all have something in common

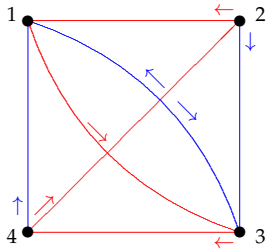
I will describe a property of permutation groups called synchronization. It turns out that "synchronizing" implies "primitive" (and even "basic", in terms of the O'Nan–Scott classification.)
But deciding which basic primitive groups are synchronizing usually involves almost no group theory, and turns into a combinatorial problem, usually an interesting (and hard) problem. So this machine gives us a big supply of interesting combinatorial problems, old and new: the three above are examples.

Automata

"Automaton" here means "finite deterministic automaton".
An automaton is a device which can be in any one of a set Ω of internal states. On the console there are a number of coloured buttons; pressing a button forces the automaton to undergo a transition, a function from Ω to itself.
Thus we can regard an automaton as an edge-coloured directed graph on Ω, with the property that there is a unique edge of each colour leaving each vertex.
An automaton is synchronizing if there is a sequence of transitions which brings it into a fixed state $\alpha \in \Omega$, from any initial state.

The dungeon

You are in a dungeon consisting of a number of rooms. Passages are marked with coloured arrows. Each room contains a special door; in one room, the door leads to freedom, but in all the others, to instant death. You have a schematic map of the dungeon, but you do not know where you are.



You can check that (Blue, Red, Blue, Blue) takes you to room 3 no matter where you start.

Algebraic formulation

Multiple button presses correspond to composition of transitions. The set of all functions generated by the given set S of transitions is closed under composition and contains the identity; thus it is a transformation monoid, the monoid generated by S.
Note that any permutation in the monoid generated by S actually lies in the group generated by the permutations in S, since a product including a non-permutation cannot be a permutation.
An automaton is synchronizing if and only if this monoid contains a constant function (an element of rank 1). A word in the generators (that is, a series of button presses which evaluates to a constant function) is called a reset word.

Applications

- Industrial robotics: pieces arrive to be assembled by a robot. The orientation is critical. You could equip the robot with vision sensors and manipulators so that it can rotate the pieces into the correct orientation. But it is much cheaper and less error-prone to regard the possible orientations of the pieces as states of an automaton on which transitions can be performed by simple machinery, and apply a reset word before the pieces arrive at the robot.
- Bioinformatics: If a soup of DNA molecules is to perform some computation, we need the molecules to be all in a known state first. We can simultaneously apply a reset word to all of them, where the transitions are induced by some chemical or biological process.

The Černý conjecture

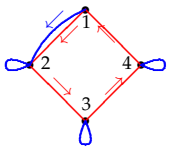
The study of synchronizing automata has been driven by the Černý conjecture, made in the 1960s and still open:

Conjecture

If an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$.

If true, this would be best possible, as the example on the next slide shows. The Černý conjecture has been proved in a few special cases, but the best general bound is cubic in n.

An example



	B	R	R	R	B	R	R	R	B
1	2	3	4	1	2	3	4	1	2
2	2	3	4	1	2	3	4	1	2
3	3	4	1	2	2	3	4	1	2
4	4	1	2	3	3	4	1	2	2

So BRRRBRRRB is a reset word of length $9 = (4-1)^2$. It can be checked that this is the shortest reset word.
Replacing the square with a regular n-gon gives examples meeting the bound for all n.

Graph homomorphisms

Graph homomorphisms

From now on, graphs are loopless, without multiple edges, and undirected.
We let $\omega(X)$, $\chi(X)$ and $\alpha(X)$ be the clique number (order of the largest clique), chromatic number (smallest number of colours in a proper coloring), and independence number (order of the largest null subgraph, or clique number of the complement) in X.
A homomorphism from a graph X to a graph Y is a map from the vertex set of X to the vertex set of Y which maps edges to edges. (A non-edge could map to a non-edge, or to an edge, or collapse to a single vertex).
Two graphs X and Y are hom-equivalent if there are homomorphisms from X to Y and from Y to X.

Homomorphisms and colorings

Proposition

- *There is a homomorphism from K_m to X if and only if $\omega(X) \geq m$.*
- *There is a homomorphism from X to K_m if and only if $\chi(X) \leq m$.*
- *A graph X is hom-equivalent to a complete graph if and only if $\omega(X) = \chi(X)$.*

The core of a graph is the smallest graph hom-equivalent to it. The third condition in the proposition is equivalent to saying that the core of X is a complete graph.

Graphs and transformation monoids

A transformation monoid on a set Ω is a collection of maps from Ω to itself which is closed under composition and contains the identity map.
For example, the endomorphisms of a graph, or of any structure, on X form a transformation monoid.
There is a strong connection between endomorphism monoids and graphs:

- Any graph X has an endomorphism monoid $\mathrm{End}(X)$.
- Given a transformation monoid S, define a graph $\mathrm{Gr}(S)$ by the rule that v and w are joined if and only if there is no element $s \in M$ mapping v and w to the same place.

Proposition

For any transformation monoid M or graph X,

- $M \leq \mathrm{End}(\mathrm{Gr}(M))$, *and* $X \leq \mathrm{Gr}(\mathrm{End}(X))$;
- $\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(M))) = \mathrm{Gr}(M)$.

The obstruction to synchronization

Theorem

A transformation monoid M on Ω is non-synchronizing if and only if there is a non-null graph X, with vertex set Ω, for which $\omega(X) = \chi(X)$ and $M \leq \mathrm{End}(X)$.

Proof.

If there is such a graph X, then no edge of X is collapsed by M, and M is non-synchronizing.
Conversely, suppose that M is non-synchronizing, and let $X = \mathrm{Gr}(M)$ and s an element of M of minimum rank. Then $M \leq \mathrm{End}(X)$, by the result on the previous slide.
No two points in the image of s can be collapsed by any element t of M (or st would have smaller rank than s); so the image is a clique in X.
Now s is a colouring, since edges map to distinct points; and clearly the size of the clique and the number of colours are both equal to the rank of s. □

Random synchronization

Conjecture

The probability that the monoid generated by two random transformations of an n-set is synchronizing tends to 1 as $n \to \infty$

A pair of transformations which do not generate a synchronizing monoid must be contained in a maximal non-synchronizing monoid. So we need to describe these objects.
By the theorem, they are full endomorphism monoids of certain graphs. I have a structural characterisation of these graphs, but haven't (yet!) been able to convert this in to bounds for the number of them and the orders of their endomorphism monoids.

Permutation groups

Permutation groups

I now turn to a case that has received a lot of attention, where M is generated by a permutation group G (a subgroup of the symmetric group on Ω) together with a single non-permutation.
Let G be a permutation group on Ω. We say that G is

- transitive if any element of Ω can be mapped by any other by some element of G, that is, there is no non-trivial G-invariant subset of Ω;
- primitive if there is no non-trivial G-invariant equivalence relation on Ω;
- 2-transitive if it acts transitively on the set of pairs of distinct elements of Ω, that is, there is no non-trivial binary relation on Ω.

A set or relation is trivial if it is invariant under the symmetric group.

Synchronizing groups

By abuse of language, we call the permutation group G synchronizing if, for any non-permutation s, the monoid $\langle G, s\rangle$ contains an element of rank 1.
Now the main question is:

Problem
Which permutation groups are synchronizing?

This approach was introduced by João Araújo and Ben Steinberg. They hoped initially that knowledge of groups would settle some more cases of the Černý conjecture; this has not happened, but many interesting developments have.

Synchronizing groups, 2

Theorem
A permutation group G on Ω is non-synchronizing if and only if there is a non-trivial G-invariant graph on the vertex set Ω with clique number equal to chromatic number.

The forward implication is immediate from the preceding theorem. Conversely, if X is a G-invariant graph with clique number and chromatic number $r > 1$, and s is an r-colouring of X with values in an r-clique, then s is an endomorphism of X, and so $\langle G, s\rangle \leq \mathrm{End}(X)$.

Synchronizing groups, 3

It follows immediately from the theorem that a 2-transitive group is synchronizing (since it preserves no non-trivial graph at all), and a synchronizing group is primitive (since an imprimitive group preserves a complete multipartite graph). Neither implication reverses.
Since the Classification of Finite Simple Groups, we know much more about primitive groups. Can we use this knowledge to learn more about synchronization?

An algorithm

Given a permutation group G on Ω, is it synchronizing?
Both primitivity and 2-transitivity can be tested in polynomial time, so we may assume that G is primitive but not 2-transitive.

- Compute the non-trivial G-invariant graphs. There are $2^r - 2$ of these, where r is the number of G-orbits on 2-sets. This is potentially exponentially large, but for many interesting groups r is much smaller than n.
- For each such graph, check whether clique number is equal to chromatic number. If we find one, G is non-synchronizing; otherwise it is synchronizing. Of course, clique number and chromatic number are hard in general, but we have highly symmetric graphs here, which shortens the calculation.

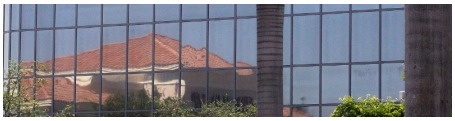
An example

Consider the symmetric group S_m acting on the set Ω of 2-element subsets of $\{1, \ldots, m\}$, with $|\Omega| = n = \binom{m}{2}$. This group is primitive if $m \geq 5$.
There are two non-trivial G-invariant graphs:

- the line graph of K_m, which has clique number $m - 1$ and chromatic number $m - 1$ if m is even, or m if m is odd;
- the Kneser graph (complement of the above), which has clique number $\lfloor m/2 \rfloor$ and chromatic number $m - 3$.

So this group is synchronizing if and only if m is odd.

Combinatorics



Combinatorics of synchronization

There has been a bit of work on deciding which primitive groups are synchronizing. It almost always turns out to depend on hard combinatorial problems.
The three introductory problems arise in considering the groups

- the general linear group $\mathrm{GL}(n,q)$, acting on the set of k-dimensional subspaces of the n-dimensional vector space;
- classical groups acting on the associated polar spaces;
- the symmetric group S_n acting on 4-subsets of $\{1,\ldots,n\}$.

Groups synchronizing non-uniform maps

The kernel type of a map s on Ω is the partition of n giving the sizes of the inverse images of points in the image of s. The map is uniform if all parts of the kernel type are equal, and non-uniform otherwise.
Araújo made the following conjecture:

Conjecture

A primitive group synchronizes every non-uniform map.

I will now describe some recent results on this using the graph endomorphism technique.

Rystsov's theorem

An early result on synchronization was proved by Rystsov:

Theorem

A permutation group G of degree n is primitive if and only if it synchronizes every map of rank $n-1$.

Araújo and I generalised this as follows. A *block of imprimitivity* for G is an equivalence class of a G-invariant equivalence relation.

Theorem

G is imprimitive with a block of imprimitivity of size at least k if and only if G fails to synchronize a map with kernel type $(k,1,\ldots,1)$.

Proof of the Theorem

Proof.

If G does not synchronize s, then $\langle G,s\rangle \leq \mathrm{End}(X)$ for some non-trivial graph X. Now the kernel class K of size k of s is collapsed to a point, so must be an independent set; so all edges from K end at points in classes of size 1, and are mapped bijectively by s. Thus, any two points in K have the same neighbour set.
Define a relation on Ω by the rule that $v \equiv w$ if v and w have the same neighbour set. This is clearly a G-invariant equivalence relation with an equivalence class of size at least k.
Conversely, if G is imprimitive with blocks of size $m \geq k$, then it preserves a complete multipartite graph X with blocks of size m; then a map collapsing k points in a block and fixing everything else is an endomorphism of X. □

An improvement

Theorem

A primitive group of degree n synchronizes every map of rank $n-2$.

Proof.

The kernel type of such a map is either $(3,1,1,\ldots,1)$ or $(2,2,1,\ldots,1)$. The first case is dealt with by the preceding theorem.
In the second case, a careful analysis of the graph shows that the permutation which interchanges the points in the two kernel classes of size 2 and fixes everything else is an automorphism of the graph. Now classical results of permutation group theory show that a primitive group containing a double transposition is symmetric or alternating if $n \geq 9$. The smaller cases can be dealt with directly. □

Maps of small rank

Theorem

A primitive group synchronizes every map of rank 2.

Proof.

A graph with an endomorphism of rank 2 is bipartite. If G preserves a non-null bipartite graph X, then

- if X is disconnected, then "same connected component" is a G-invariant equivalence relation;
- if X is connected, then "same bipartite block" is a G-invariant equivalence relation.

□

Maps of small rank, 2

By similar arguments, we showed

Theorem
A primitive group synchronizes every non-uniform map of rank 3 *or* 4.

Proof.
If a monoid M contains a transitive permutation group G, then an element of minimal rank in M is uniform. So there is nothing to prove unless the non-uniform map s has rank 4 and the minimal rank is 3, in which case the kernel partition of s splits just one kernel class of a partition of minimal rank. In general, if this condition holds, we show that G is imprimitive. □

What's special about primitive graphs?

An interesting fact arises from the above proof.
A primitive graph is a graph admitting an automorphism group which acts primitively on the vertices. Apart from symmetry, what is special about primitive graphs?
It is easy to see that:

Theorem
Every finite graph occurs as an induced subgraph of some primitive graph.

The argument about synchronizing gives the following small result in the other direction:

Theorem
Let X be a primitive graph with chromatic number r. Then X does not have an induced subgraph isomorphic to K_{r+1} minus an edge.

Can any more be said?